UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/091,740	03/06/2002	Travis J. Parry	10013768-1	8466

7590 01/18/2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
HOMAYOUNMEHR, FARID	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/091,740	PARRY, TRAVIS J.	
	Examiner	Art Unit	
	Farid Homayounmehr	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 October 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-14,17-30,33-35,37 and 39-41* is/are pending in the application.

4a) Of the above claim(s) *3, 15,16,31,32,36 and 38* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2, 4-14, 17-30, 33-35, 37, 39-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. No claim was amended by the applicant.
4. No new claim was added by the applicant.
5. Claims 1, 2, 4-14, 17-30, 33-35, 37, 39-41 have been considered.
6. Claims 3, 15, 16, 31, 32, 36, and 38 have been cancelled by the applicant.
7. All other claims are rejected.

Response to Arguments

8. Applicant's arguments filed 10/24/2006, relative to allowability of claims 1, 2, 4-14, 17-30, 33-35, 37, 39-41 has been fully considered, but is not persuasive.

8.1. Claim 1:

With regard to claim 1, applicant argues that Schwartz fails to teach or suggest searching for a firewall associated with a destination at a remote network, as it only

teaches searching a firewall on a local network where the device is also connected. However, as described in the previous office action, Schwartz does disclose all the elements of the claim, including the search of a firewall associated with a destination at a remote network. Cited paragraph 0025 reads: "The ability to pass through the firewall is where the present invention for firewall traversal is applicable. One skilled in the art will recognize that bi-directional communications is readily possible once the firewall has been traversed". Therefore, the client shown in Fig. 3 may have to pass the firewall associated with the appliances in the remote network to control them. This is suggested in paragraph 25 with the example of accessing the music stored on a site behind a firewall. Therefore, Schwartz invention is about accessing devices in a remote network behind an associated firewall, as well as bypassing a firewall protecting the local area network where the client machine is located (bi-directional). In addition, in the embodiment described in paragraph 39-40, Schwartz's system clearly communicates with a remote site beyond a firewall. Therefore, applicant's argument that Schwartz system only teaches communication through a local network and local firewall is not persuasive.

Applicant further argues that Schwartz fails to teach a request to transmit data includes the primary address of the destination that is used if a firewall is not detected and a secondary address of the destination if the firewall is detected. However, Schwartz does try a primary address and if it fails a connection it tries the second address. It is true that Schwartz won't try the primary address again if it fails, but clearly tries it the first time,

which was before the connection failed. Therefore, the address of the primary and secondary protocols must be received by the device that initiates the connection.

Applicant further agues that Schwartz fails to teach "a request to transmit data comprises both the primary address and secondary address of the destination". However, Schwartz tries the primary address and if it fails, tries the secondary address. Therefore, the address of the primary and secondary protocols must be received by the device that initiates the connection. As further clarification, note that paragraph 30 describes opening a connection made possible by a software using different protocols (as described in blocks 402, 408, 412) which configures an Ethernet Adapter card. Therefore, the software configuring the Ethernet adapter card handles a request to establish communication, which involves attempting different addresses associated with different protocols until the communication is established. Paragraphs 39-40 describe different ways to determine the addresses associated with the alternative protocols. No matter how addresses are determined, the device which establishes the communication, must receive the addresses to be able to communicate using the associated protocols. This matches the requirements of claim 1. Note that based on claim 1 language, the firewall prohibits communication via a communication protocol and allows communication via a secondary communication protocol. This is different than the limitation which requires searching for firewalls configured to prohibit communication via the primary communication protocol associated with the first address identified in the request, and allow communication via the secondary communication

protocol associated with the secondary address identified in the request. In other words, the claim limitation does not require the search for a firewall prohibiting or allowing communication based on the data in the request.

8.2. Claims 2 and 4-13:

Based on the above discussion, applicant argument relative to allowability of claims 2 and 4-13 based on their dependency on claim 1 is not persuasive.

8.3. Claims 14, 17-30, 33-35, 37, 39-41:

Applicant's argument relative to claims 14, 17-30, 33-35, 37, 39-41 is substantially the same as their argument relative to claims 1, 2, 4-13 above, and according to the above discussion is not persuasive.

9. In view of the above, applicants' amendments have failed to put the claims in the condition of allowability. Claims rejection is as follows:

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 2, 4-14, 17-30, 33-35, 37, 39-41 are rejected under 35 U.S.C. 102(e) as being anticipated by Schwartz (US Patent Application Publication US 2002/0199114 A1).

10.1. As per claim 1, Schwartz is directed to a method of transmitting data across a firewall (paragraph [0013] line 1), the method comprising:
receiving a request to transmit data to a destination (paragraph [0028], where the client's attempt to open a connection discloses a request to transmit data); searching for a firewall associated with the destination (paragraph [0028] lines 8 to 11) at a remote network (for example, Fig. 3 item 314-5 is in network 311, which is associated with firewall 310, which is remote to client 308-1. See also paragraph 25), the firewall being configured to prohibit communication to the destination at a remote network via a primary communication protocol (Fig 4 and paragraph [0029] as disclosed by TCP port x, where the connection is not established), and allow communication to the destination via a secondary communication protocol (paragraph [0003], as it is describing the general functionality of a firewall); if the firewall is detected, automatically configuring the data for communication with the secondary communication protocol (paragraph [0029] line 1 to 5); and transmitting the data to the destination by utilizing the secondary communication protocol (paragraph [0029]), wherein the request to transmit data to the

destination comprises a primary address to the destination related to the primary communication protocol, and a secondary address to the destination related to the secondary communication protocol (paragraph [0028] and [0029], where, after the failure to connect via TCP (example of a primary protocol), the device tries to open a HTTP connection (example of the secondary protocol), and Schwartz claims 2 to 4 wherein the primary and secondary protocols use predefined addresses to initiate the connection and paragraphs [0040] and [0041], where the addresses are provided by the address database to the Communication Subsystem as communication parameters).

10.2. As per claim 2, Schwartz continues to teach the method of claim 1, further comprising: transmitting the data to the destination by utilizing the primary communication protocol if the firewall is not detected (paragraph [0029] line 1 to 5).

10.3. Claim 3 has been cancelled by the applicant.

10.4. As per claim 4, Schwartz discloses the method of claim 1, wherein the destination is a printer and a print job comprises the data that is requested to be transmitted. Printer is a computer peripheral that puts text or a computer-generated image on paper or on another medium, such as transparency film. Local printers communicate with the network via a PC, and network printers are directly connected to the network. Schwartz clearly discloses display and I/O devices (Fig. 2, item 220 and paragraph [0016]) as the parts comprising the clients' computer. In addition, Schwartz discloses traditionally

connected devices, which are devices configurable to communicate through the firewall, and non-traditional devices, which are devices that must be connected to another device (e.g. a PC) in order to communicate (paragraph [0024). Traditionally connected devices and non-traditional devices receive jobs in form of data directly or indirectly form the network, correspondingly. As indicated in Fig. 3, both traditionally connected and non-traditional devices are behind the firewall, and are disclosed as destinations for data to be transmitted across the firewall. Therefore, the Examiner asserts that Schwartz discloses the feature.

10.5. As per claim 5, Schwartz discloses the method of claim 1, wherein searching for the firewall comprises pinging the primary address of the desired location. Pinging is sending out a small amount of information, or a packet, to a destination connected to the network, and examining the response to determine if the destination is responsive to network requests. Schwartz discloses initiation of a first connection and evaluating the connection for the response from the remote system (claim 1). More specifically, Pinging is sending out ICMP Echo Request Packets. Schwartz discloses ICMP as one of the protocols to initiate the first connection (claim 2). Therefore, the Examiner asserts that it discloses the feature.

10.6. As per claim 6, Schwartz discloses the method of claim 2, wherein searching for the firewall comprises:

scanning the desired location to find an open port, the open port being related

to the primary communication protocol; and detecting the firewall, if present, upon not finding the open port. Scanning is examining sequentially, part by part. As disclosed in Fig. 4, and described in paragraph [0029] the device that is transmitting the data examines the firewall by initiating connections using TCP, HTTP, and other options sequentially until a connection is established (Open port found). Therefore, it discloses the feature.

10.7. As per claim 7, Schwartz discloses the method of claim 2, wherein searching for the firewall comprises:

attempting to transmit the data via the primary communication protocol, such that a failure to successfully transmit the data via the primary communication protocol would signify the firewall is present. As described in Schwartz paragraph [0027], attempting to initiate a connection, involves transmitting data. Schwartz maintains that depending on the type of the communication protocol, different set of steps and data exchanges may be involved to determine whether a connection is established. Furthermore, when data transmission is unsuccessful, Schwartz tries another protocol (Fig. 4), which indicates that a firewall blocking the primary transmission is detected. Therefore it discloses the feature.

10.8. As per claim 8, Schwartz discloses the method of claim 2, wherein the primary communication protocol is any one or combination of the following:

the Hyper-Text Transfer Protocol (HTTP), the Transfer Control Protocol (TCP), the Internet Protocol (IP), the File Transfer Protocol (FTP), and the User Datagram Protocol (UDP). Schwartz clearly discloses primary communication protocols HTTP, TCP and UDP in claim 2, and IP in claim 10.

Schwartz recognizes and mentions FTP packets as another example of protocol data units examined and evaluated by firewalls (paragraph [0005]). Schwartz also refers to RFCs as other potential standards and protocols to be used as primary communication protocol (paragraph [0045]), one of which is RFC 959, The File Transfer Protocol. Therefore, the Examiner asserts that Schwartz discloses the feature.

10.9. As per claim 9, Schwartz discloses the method of claim 1, wherein the secondary communication protocol is an
electronic mail (email) protocol (as disclosed in paragraph [0045], referring to RFCs for a list of potential protocols for communication, one of which is RFC 821, Simple Mail Transfer Protocol), and the secondary address is an email address (when SMTP is used as secondary communication protocol, an email address must be selected as the destination address); and further wherein automatically configuring the data for communication comprises: generating an email; addressing the email to the secondary address; and populating the email with pertinent information that correlates to the data. Data must be configured appropriately before transferred using any communication protocol. When email is used as the communication protocol, it is well

known that an email must be generated, addressed to the email address of the destination, and the data must be configured in the format that is suitable for email.

10.10. As per claim 10, Schwartz discloses the method of claim 9, wherein automatically configuring the data for communication further comprises: placing the data in the email (see section 3.9 above).

10.11. As per claim 11, Schwartz discloses the method of claim 9, wherein automatically configuring the data for communication further comprises: attaching the data to the email, the data being stored in a file (see section 3.9 above. Attachment is a well known way to configure data for transfer using email).

10.12. As per claim 12, Schwartz is directed to the method of claim 9, wherein the information that is populated in the email comprises a reference to a remote location where the data is stored and is accessible from the destination (in this case the data transmitted across the firewall is simply the data identifying the location of another data. Allowing access to data that is already accessible to the destination by identifying the location of the data is well-known in the art).

10.13. As per claim 13, Schwartz discloses the method of claim 1, wherein the secondary communication protocol is the File Transfer Protocol (FTP) and the secondary address is an FTP address. Schwartz recognizes and mentions FTP packets

as another example of protocol data units examined and evaluated by firewalls (paragraph [0005]). Schwartz also refers to RFCs as other potential standards and protocols to be used as primary communication protocol (paragraph [0045]), one of which is RFC 959, The File Transfer Protocol. Therefore, the Examiner asserts that Schwartz discloses the feature.

10.14. As per claim 14, Schwartz is directed a system for rerouting the transmission of data to avoid a firewall (paragraph [0013] line 1), the system comprising: a transmission device configured to search for a firewall protecting a destination (paragraph [0028], where the client's attempt to open a connection discloses a request to transmit data) at a remote network (for example, Fig. 3 item 314-5 is in network 311, which is associated with firewall 310, which is remote to client 308-1. See also paragraph 25), the firewall at the remote network being configured to prohibit communication to the destination via a primary communication protocol searching for a firewall associated with the destination (paragraph [0028] lines 8 to 11), the firewall being configured to prohibit communication to the destination via a primary communication protocol (Fig 4 and paragraph [0029] as disclosed by TCP port x, where the connection is not established), and allow communication to the destination via a secondary communication protocol (paragraph [0003], as it is describing the general functionality of a firewall), the transmission device is further configured to, upon detection of the firewall, automatically configure the data for communication over the secondary communication protocol (paragraph [0029] line 1 to 5) and transmit the data by utilizing the secondary communication protocol

(paragraph [0029]), wherein the transmission device is further configured to receive a request to transmit data to the destination and the request comprises at least the following: a primary address and a secondary address of the destination, the primary address being related to the primary communication protocol, and the secondary address being related to the secondary communication protocol (paragraph [0028] and [0029], where, after the failure to connect via TCP (example of a primary protocol), the device tries to open a HTTP connection (example of the secondary protocol), and Schwartz claims 2 to 4 wherein the primary and secondary protocols use predefined addresses to initiate the connection and paragraphs [0040] and [0041], where the addresses are provided by the address database to the Communication Subsystem as communication parameters), and wherein the transmission device is further configured to, upon not detecting the firewall, transmit the data to the destination by utilizing the primary transmission protocol (claim 1 indicates evaluation of the first connection, and trying the second if the first one was unsuccessful. Thus, if the evaluation shows that the transmission was successful, no firewall is detected and the transmission was done using the primary protocol).

10.15. Claim 15 is cancelled by the applicant.

10.16. Claim 16 is cancelled by the applicant.

10.17. As per claim 17, Schwartz is directed to the system of claim 14, wherein the transmission device is further configured to search for a firewall by scanning the destination to find an open port, the open port being related to the primary communication protocol, upon not finding the open port, the firewall is detected. Scanning is examining sequentially, part by part. As disclosed in Fig. 4, and described in paragraph [0029] the device examines the firewall by initiating connections using TCP, HTTP, and other options sequentially until a connection is established (Open port found). Therefore, it discloses the feature.

10.18. As per claim 18, Schwartz is directed to the system of claim 14, wherein the transmission device is further configured to search for a firewall by pinging the primary address of the destination. Pinging is sending out a small amount of information, or a packet, to a destination connected to the network, and examining the response to determine if the destination is responsive to network requests. Schwartz discloses initiation of a first connection and evaluating the connection for the response from the remote system (claim 1). More specifically, Pinging is sending out ICMP Echo Request Packets. Schwartz discloses ICMP as one of the protocols to initiate the first connection (claim 2). Therefore, the Examiner asserts that it discloses the feature.

10.19. As per claim 19, Schwartz is directed to the system of claim 14, wherein the transmission device is further configured to search for a firewall by attempting to transmit the data via the primary communication protocol, such that a failure to

successfully transmit the data via the primary communication protocol would signify the firewall is present. As described in paragraph [0027], attempting to initiate a connection, involves transmitting data. Schwartz maintains that depending on the type of the communication protocol, different set of steps and data exchanges may be involved to determine whether a connection is established. Furthermore, when data transmission is unsuccessful, Schwartz tries another protocol (Fig. 4), which indicates that a firewall blocking the primary transmission is detected. Therefore it discloses the feature.

10.120. As per claim 20 Schwartz discloses the system of claim 14, wherein the secondary communication protocol is an electronic mail (email) protocol (as disclosed in paragraph [0045], referring to RFCs for a list of potential protocols for communication, one of which is RFC 821, Simple Mail Transfer Protocol).

10.21. As per claim 21, Schwartz discloses the system of claim 20, wherein the secondary address is an email address (when SMTP is used as secondary communication protocol, an email address must be used as the destination address) and wherein the transmission device is further configured to automatically configure communication by: generating an email; addressing the email to the secondary address; and populating the email with pertinent information that correlates to the data. When email is used as the communication protocol, an email must be generated, addressed to the email address of the destination, and the data must be configured in the format that is suitable for email.

10.22. As per claim 22, Schwartz discloses the system of claim 21, wherein the transmission device is further configured to automatically configure the data for communication by placing the data in the email (see section 3.21 above).

10.23. As per claim 23, Schwartz discloses the system of claim 21, wherein the transmission device is further configured to automatically configure the data for communication by attaching the data to the email, the data being stored in a file (see section 3.21 above. Attachment is a well know method to configure data for transfer using email).

10.24. As per claim 24, Schwartz is directed to the system of claim 21, wherein the information that is populated in the email comprises a reference to a remote location where the data is stored and is accessible from the destination (in this case the data transmitted across the firewall is simply the data identifying the location of another data. Allowing access to data that is already accessible to the destination by identifying the location of the data is well-known in the art).

10.25. As per claim 25, Schwartz is directed to the system of claim 14, wherein the secondary communication protocol is the File Transfer Protocol (FTP) and wherein the secondary address is an FTP address. Schwartz recognizes and mentions FTP packets as another example of protocol data units examined and evaluated by firewalls

(paragraph [0005]). Schwartz also refers to RFCs as other potential standards and protocols to be used as primary communication protocol (paragraph [0045]), one of which is RFC 959, The File Transfer Protocol. Therefore, the Examiner asserts that Schwartz discloses the feature.

10.26. As per claim 26, Schwartz discloses the system of claim 14, wherein the primary communication protocol is any one or combination of the following: the Hyper-Text Transfer Protocol (HTTP), the Transfer Control Protocol (TCP), the Internet Protocol (IP), the File Transfer Protocol (FTP), and the User Datagram Protocol (UDP). Schwartz clearly discloses primary communication protocols HTTP, TCP and UDP in claim 2, and IP in claim 10.

Schwartz recognizes and mentions FTP packets as another example of protocol data units examined and evaluated by firewalls (paragraph [0005]). Schwartz also refers to RFCs as other potential standards and protocols to be used as primary communication protocol (paragraph [0045]), one of which is RFC 959, The File Transfer Protocol. Therefore, the Examiner asserts that Schwartz discloses the feature.

10.27. As per claim 27, Schwartz discloses the system of claim 14, further comprising: a recipient device configured to be the destination, the recipient device further configured to communicate with the primary and secondary communication protocol (Fig. 4 and paragraph [0027]).

10.28. As per claim 28, Schwartz is directed to the system of claim 27, wherein the recipient device is a printer and a print job comprises the data. Printer is a computer peripheral that puts text or a computer-generated image on paper or on another medium, such as transparency film. Local printers communicate with the network via a PC, and network printers are directly connected to the network. Schwartz clearly discloses display and I/O devices (Fig. 2, item 220 and paragraph [0016]) as the parts comprising the clients' computer. In addition, Schwartz discloses traditionally connected devices, which are devices configurable to communicate through the firewall, and non-traditional devices, which are devices that must be connected to another device (e.g. a PC) in order to communicate (paragraph [0024). Traditionally connected devices and non-traditional devices receive jobs in form of data directly or indirectly form the network, correspondingly. As indicated in Fig. 3, both traditionally connected and non-traditional devices are behind the firewall, and are disclosed as destinations for data to be transmitted across the firewall. Therefore, the Examiner asserts that Schwartz discloses the feature.

10.29. As per claim 29, Schwartz is directed to a transmission device configured to transmit data to a destination, the transmission device comprising: means for transmitting the data to a destination at a remote network (for example, Fig. 3 item 314-5 is in network 311, which is associated with firewall 310, which is remote to client 308-1. See also paragraph 25) by utilizing a secondary communication protocol (paragraph

[0029]), means for searching for a firewall at a remote network (paragraph [0028] lines 8 to 11), the firewall being configured to prohibit communication to the destination by a primary communication protocol (Fig 4 and paragraph [0029] as disclosed by TCP port x, where the connection is not established), and allow communication to the destination via the secondary communication protocol (paragraph [0003], as it is describing the general functionality if a firewall); and means for automatically configuring the data for communication for the secondary communication protocol upon detecting the firewall (paragraph [0029] line 1 to 5) and

means for receiving a request to transmit the data to the destination, wherein the request comprises at least the following:

a primary address to the destination related to the primary communication protocol, and a secondary address to the destination related to the secondary communication protocol (paragraph [0028] and [0029], where, after the failure to connect via TCP (example of a primary protocol), the device tries to open a HTTP connection (example of the secondary protocol), and Schwartz claims 2 to 4 wherein the primary and secondary protocols use predefined addresses to initiate the connection and paragraphs [0040] and [0041], where the addresses are provided by the address database to the Communication Subsystem as communication parameters).

10.30. As per claim 30, Schwartz is directed to the device of claim 29, further comprising means for transmitting the data by utilizing the primary communication

protocol, wherein upon not detecting the firewall, the data is transmitted by utilizing the primary communication protocol (paragraph [0029] line 1 to 5).

10.31. Claim 31 is cancelled by the applicant.

10.32. Claim 32 is cancelled by the applicant.

10.33. As per claim 33, Schwartz is directed to the device of claim 30, wherein the secondary communication protocol is an electronic mail (email) protocol (as disclosed in paragraph [0045], referring to RFCs for a list of potential protocols for communication, one of which is RFC 821, Simple Mail Transfer Protocol).

10.34. As per claim 34, Schwartz is directed to the device of claim 30, wherein the secondary address is an email address (when email is the means to transfer information, and SMTP is used as secondary communication protocol, an email address must be used as destination address), and wherein the means for automatically configuring the data for communication for the secondary communication protocol comprises: means for generating an email, means for addressing the email to the secondary address; means for populating the email with pertinent information that correlates to the data; and means for populating the email with the data . Data must be configured appropriately before transferred using any communication protocol. When email is used as the means to transfer data an email must be generated, addressed to

the email address of the destination, and the data must be configured in the format that is suitable for email.

10.35. As per claim 35, Schwartz is directed to a data transmission program stored on a computer-readable medium (paragraph [0014]), the transmission program comprising: logic configured to facilitate the transmission of data to a remote network (item 314-5 in the network 311, which is remote from client 308-1) by utilizing a secondary communication protocol (paragraph [0029]); logic configured to search for a firewall (paragraph [0028] lines 8 to 11) at a remote network (for example, Fig. 3 item 314-5 is in network 311, which is associated with firewall 310, which is remote to client 308-1. See also paragraph 25), wherein the firewall is configured to prohibit communication to a recipient device at a remote network via a primary communication protocol and allow a communication via the secondary protocol (paragraph [0028])
and logic configured to automatically configure communication for the secondary communication protocol upon detecting the firewall (paragraph [0029]) and
logic configured to receive a request to transmit the data to the recipient device, the request comprising at least of the following:
a primary address to the destination related to the primary communication protocol, and a secondary address to the destination related to the secondary communication protocol (paragraph [0028] and [0029], where, after the failure to connect via TCP (example of a primary protocol), the device tries to open a HTTP connection (example of the secondary protocol), and Schwartz claims 2 to 4 wherein the primary and

secondary protocols use predefined addresses to initiate the connection and paragraphs [0040] and [0041], where the addresses are provided by the address database to the Communication Subsystem as communication parameters).

10.36. Claim 36 is cancelled by the applicant.

10.35. As per claim 37, Schwartz is directed to the program of claim 35, further comprising logic configured to facilitate the transmission of the data by utilizing the primary communication protocol, wherein upon not detecting the firewall, the data is transmitted by utilizing the primary communication protocol (paragraph [0029] line 1 to 5).

10.38. Claim 38 is cancelled by the applicant.

10.39. As per claim 39, Schwartz is directed to the program of claim 35, wherein the secondary address is an electronic mail (email) address (which must be the case when communication protocol is email) and the secondary communication protocol is an email protocol (as disclosed in paragraph [0045], referring to RFCs for a list of potential protocols for communication, one of which is RFC 821, Simple Mail Transfer Protocol); and wherein the logic configured to automatically configure the data for communication for the secondary communication protocol comprises: logic configured to generate an email; logic configured to address the email to the secondary address; logic configured

to populate the email with pertinent information that correlates to the data; and logic configured to populate the email with the data. Data must be configured appropriately before transferred using any communication protocol. When email is used as the communication protocol, it would be obvious to a person with ordinary skills in the art that an email must be generated, addressed to the email address of the destination, and the data must be configured in the format that is suitable for email.

10.40. As per claim 40, Schwartz is directed to the program of claim 35, wherein the secondary communication protocol is the File Transfer Protocol (FTP) and the secondary address is an FTP address. Schwartz recognizes and mentions FTP packets as another example of protocol data units examined and evaluated by firewalls (paragraph [0005]). Schwartz also refers to RFCs as other potential standards and protocols to be used as primary communication protocol (paragraph [0045]), one of which is RFC 959, The File Transfer Protocol. Therefore, the Examiner asserts that Schwartz discloses the feature.

10.41. As per claim 41, Schwartz is directed to the program of claim 35, wherein the primary communication protocol is any one or combination of the following: the Hyper-Text Transfer Protocol (HTTP), the Transfer Control Protocol (TCP), the Internet Protocol (IP), the File Transfer Protocol (FTP), and the User Datagram Protocol (UDP). Schwartz clearly discloses primary communication protocols HTTP, TCP and UDP in claim 2, and IP in claim 10.

Schwartz recognizes and mentions FTP packets as another example of protocol data units examined and evaluated by firewalls (paragraph [0005]). Schwartz also refers to RFCs as other potential standards and protocols to be used as primary communication protocol (paragraph [0045]), one of which is RFC 959, The File Transfer Protocol. Therefore, the Examiner asserts that Schwartz discloses the feature.

Conclusion

9. **THIS ACTION IS MADE FINAL,** as no new ground of rejection is included. See MPEP § 7.39. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is (571)

272-3739. The examiner can be normally reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr F.H.

1/3/2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100